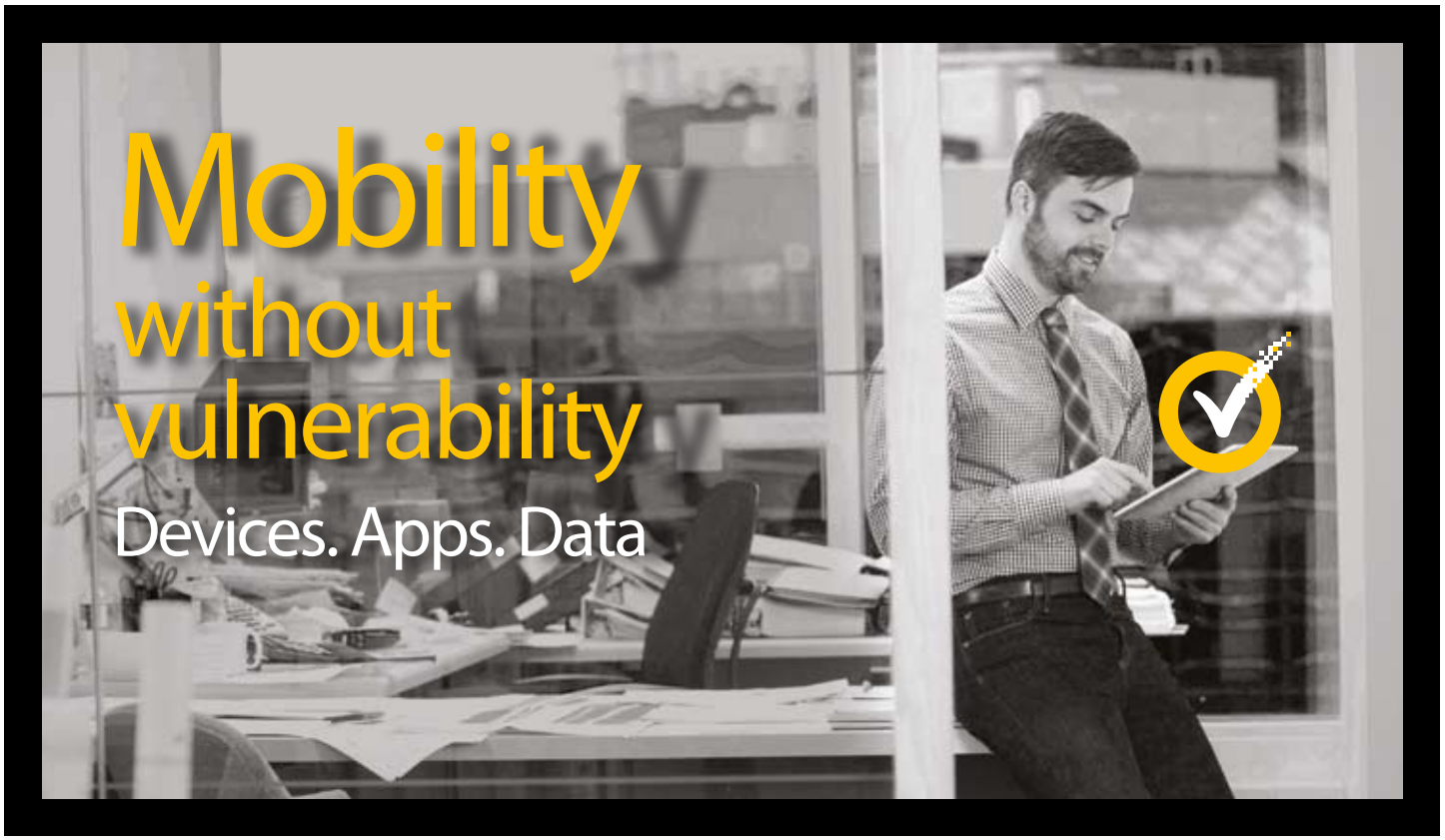
Symantec. Confidence in a connected world .



What are the key security considerations for mobile computing?

Here are our top 5 – plus some useful advice

The freedom to do business anywhere, anytime can ramp up productivity, increase employee satisfaction and deliver a competitive edge.

Here's what you should be watching out for in this new flexible world of remote access, Bring Your Own Device and cloud computing.

1. Control and protect your mobile apps and data

When your employees are working outside the corporate firewall, it's important to make sure that apps and data are secure. That's when they're most at risk of theft or deletion by from malicious hackers, or disaffected or careless employees.

Mobile apps are the primary method to access, view, store, and transmit data, and with more apps in use, there is more sensitive data on mobile devices. So both apps and data must have controls and protection appropriate to your company and industry.

2. Make sure users are who they say they are

It sounds obvious, but the people, apps and devices that connect to and access business assets MUST at all times be identified as authorized business participants. You should have robust solutions in place to validate user identity.

No ifs, no buts – identity is the first and most important component in any IT strategy. This is especially true where mobility is concerned, as device and cloud access is inherently less strict than the controls routinely applied to corporate networks.

3. Business asset or personally-owned, cover every mobile device

Any device that accesses business assets and connects to your network must be managed and secured according to applicable company policies and industry regulations. That's especially true of company-owned devices that are corporate-liable.

If you don't already have them, establish appropriate mobile policies; and make sure that you have robust protection in place to secure devices, apps and data.

4. Secure all your endpoints, and simplify multi-platform complexity

Bring Your Own Device has taken off like wildfire, with smartphones, tablets and laptops on a wide variety of platforms including Android, Blackberry and iOS. Make sure you don't get burned attempting to deal with each platform through a point solution.

Far less expensive – and less complex – is to have comprehensive threat protection across the board. That means you safeguard every device, whether company-liable or personally owned, and the apps and data on them. Good threat protection should protect against external attacks, rogue apps, unsafe browsing, theft and even poor battery use.

5. Keep your business secrets, secret

Collaboration between individuals, workgroups, even companies, is the norm in business today. That makes the cloud an obvious and simple solution for distributing and synchronising information between devices.

Secure your file sharing with a suitable program and protect your company's privacy with full administrative control over distribution and access to business documents on your network – with special emphasis on the cloud.

And finally, think like a hacker

The bad guys are smart and determined. Whether their intentions are malicious – with malware attacks including Trojan horses and worms to cause damage, loss or corruption of sensitive data – or they are set on financial gain through 'phishing' or targeted attacks, they are dangerous.

However, they are not invincible. Picture yourself in a hacker's shoes and identify any weaknesses in your network and your mobile activities. By putting appropriate security measures in place and rigorously maintaining your defences, you can expect to conduct business as usual.

Symantec protects the world's people and information.

Our solutions for enterprise mobility span User & App Access, App & Data Protection, Device Management, Threat Protection and Secure File Sharing – all from a single vendor.

For more information visit www.symantec.co.uk/mobility

Confidence in a connected world. Symantec